On connectivity in a general random intersection graph

Jun Zhao

Dept. of ECE
Carnegie Mellon University
junzhao@alumni.cmu.edu

August 15, 2015

Abstract

There has been growing interest in studies of general random intersection graphs. In this paper, we consider a general random intersection graph $\mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n)$ defined on a set $\mathcal{V}_n$ comprising n vertices, where $\overrightarrow{\alpha}$ is a probability vector $(a_1, a_2, \ldots, a_m)$ and $\overrightarrow{K_n}$ is $(K_{1,n}, K_{2,n}, \ldots, K_{m,n})$. This graph has been studied in the literature [10,11,20,29] including a most recent work by Yağan [20]. Suppose there is a pool $\mathcal{P}_n$ consisting of P_n distinct objects. The n vertices in $\mathcal{V}_n$ are divided into m groups $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$. Each vertex v is independently assigned to exactly a group according to the probability distribution with $\mathbb{P}[v \in \mathcal{A}_i] = a_i$, where $i = 1, 2, \ldots, m$. Afterwards, each vertex in group $\mathcal{A}_i$ independently chooses $K_{i,n}$ objects uniformly at random from the object pool $\mathcal{P}_n$. Finally, an undirected edge is drawn between two vertices in $\mathcal{V}_n$ that share at least one object. This graph model $\mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n)$ has applications in secure sensor networks and social networks. We investigate connectivity in this general random intersection graph $\mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n)$ and present a sharp zero-one law. Our result is also compared with the zero-one law established by Yağan [20].

Keywords— Connectivity, general random intersection graph, isolated vertex, zero-one law.

1 Introduction

Recently, there has been considerable attention in analyzing random intersection graphs [1–3,5,6,8,9,17–19,22, 26–29]. In a random intersection graph, each vertex is assigned to a set of items in a random manner, and two vertices have an undirected edge in between if and only if they have at least some number of items in common. In a specific model for a *uniform* random intersection graph [2,17,29], each vertex is independently assigned the same number of objects uniformly at random from a pool comprising different objects, and an undirected edge is drawn between two vertices that share at least one object. In the literature, the uniform random intersection graph model has been extensively studied [2,3,5,8,9,17,18,22,26–28], and there has been an increasing interest in investigating *general* random intersection graphs [10, 11, 20, 29].

In this paper, we look at a general random intersection graph defined as below. We consider a graph defined on a set $\mathcal{V}_n$ with n vertices. All vertices are divided into m different groups $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$. Specifically, each vertex $v \in \mathcal{V}_n$ is independently assigned to exactly one group according to the following probability distribution[1]: $\mathbb{P}[v \in \mathcal{A}_i] = a_i$ for $i = 1, 2, \ldots, m$, where m is a positive constant integer, and $a_i|_{i=1,2,\ldots,m}$ are positive constants satisfying the natural condition $\sum_{i=1}^{m} a_i = 1$ (note that m and $a_i|_{i=1,2,\ldots,m}$ do not scale with n). The edge set is built as follows. To begin with, assume that there exists a pool $\mathcal{P}_n$ consisting of P_n distinct objects. Then for $i = 1, 2, \ldots, m$, each vertex in group $\mathcal{A}_i$ independently chooses $K_{i,n}$ objects uniformly at random from the object pool $\mathcal{P}_n$, where $1 \leq K_{i,n} \leq P_n$. Finally, any two vertices in $\mathcal{V}_n$ have an undirected edge in between if and only if they share at least one object. With vectors $\overrightarrow{\alpha}$ and $\overrightarrow{K_n}$ given by $\overrightarrow{\alpha} = (a_1, a_2, \ldots, a_m)$ and $\overrightarrow{K_n} = (K_{1,n}, K_{2,n}, \ldots, K_{m,n})$, respectively, we denote the graph constructed above by $\mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n)$. This

[1]We summarize the notation and convention as follows. Throughout the paper, $\mathbb{P}[\cdot]$ denotes a probability and $\mathbb{E}[\cdot]$ stands for the expectation of a random variable. All limiting statements are understood with $n \to \infty$. We use the standard asymptotic notation $o(\cdot), O(\cdot), \Omega(\cdot), \omega(\cdot), \Theta(\cdot), \sim$. In particular, for two positive sequences f_n and g_n, the relation $f_n \sim g_n$ means $\lim_{n\to\infty}(f_n/g_n) = 1$. Also, "ln" stands for the natural logarithm function, and "$|\cdot|$" can denote the absolute value as well as the cardinality of a set.

graph has been investigated in the literature [10, 11, 20, 29]. For such a graph $\mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n)$, we establish a zero-one law for connectivity:

For a graph $\mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n)$ under $P_n = \Omega(n)$ and $\omega(1) = K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{m,n} = o(\sqrt{P_n})$, if there exists a sequence β_n satisfying $|\beta_n| = o(\ln n)$ such that

$$\sum_{j=1}^{m} \left\{ a_j \left[1 - \frac{\binom{P_n - K_{1,n}}{K_{j,n}}}{\binom{P_n}{K_{j,n}}} \right] \right\} = \frac{\ln n + \beta_n}{n}, \tag{1}$$

then it holds that

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c} \mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n) \\ \textit{is connected.} \end{array} \right] = \begin{cases} 0, & \textit{if } \lim\limits_{n\to\infty} \beta_n = -\infty, \quad (2a) \\ 1, & \textit{if } \lim\limits_{n\to\infty} \beta_n = \infty. \quad (2b) \end{cases}$$

For a general random intersection graph $\mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n)$, (2a) (resp., (2b)) present a zero-law (resp., one-law) for connectivity. This zero-one law indicates that a *critical* scaling for connectivity in a general random intersection graph $\mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n)$ is to have the quantity in the left hand side of (1) being $\frac{\ln n}{n}$, and β_n in measures how much this quantity deviates from the critical value $\frac{\ln n}{n}$. Moreover, the zero-one law is *sharp* since it suffices to have an unbounded deviation β_n for (2a) and (2b); e.g., β_n could be $\pm\Theta(\ln n \ln n)$, $\pm\Theta(\ln n \ln n \ln n)$, etc. (We also note that our result has a condition $|\beta_n| = o(\ln n)$ for the proof to get through.)

We explain below applications of our result to secure wireless sensor networks and social networks. In large-scale wireless sensor networks, an recognized approach to secure sensor communications is random key predistribution, where sensors are equipped with cryptographic keys before deployment and uses the shared keys to establish secure communication after deployment. Among various random key predistribution schemes, a scheme proposed by Eschenauer and Gligor (EG) [8] has gained the most attention. In the EG scheme, the memory of each sensor before deployment has a number of cryptographic keys selected uniformly at random from a common pool comprising distinct keys, and two sensors are able to communicate securely if they share at least one key. As explained below, a general random intersection graph $\mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n)$ represents the topology of a secure sensor network employing a variation of the EG scheme in consideration of sensor heterogeneity, with the notion of an object in the graph construction is specified as a cryptographic key. In a secure sensor network, all n sensors are classified into m groups $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$. Sensors in distinct groups may have different memory resources and thus are equipped with different number of keys. Specifically, for $i = 1, 2, \ldots, m$, each sensor in group $\mathcal{A}_i$ independently selects $K_{i,n}$ keys uniformly at random from a pool $\mathcal{P}_n$ comprising P_n different keys. Clearly, our result provides an analytical guideline on how to choose network parameters so that the secure sensor networks is connected with high probability. We further explain that the conditions $P_n = \Omega(n)$ and $\omega(1) = K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{m,n} = o(\sqrt{P_n})$ are practical in secure sensor networks. First, $K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{m,n}$ are assumed without loss of generality. Second, the key pool size P_n grows at least linearly with the number of sensors n and the number of keys on a sensor increases with n becomes larger to have reasonable resiliency against sensor capture attacks [7, 21, 26], so $P_n = \Omega(n)$ are $K_{1,n} = \omega(1)$ both practical. Finally, since the number of keys on a sensor is often bounded above by a polylogarithmic function of n since sensors have limited memory to store keys [7, 21, 26] and P_n is $\Omega(n)$ as mentioned above, $K_{m,n} = o(\sqrt{P_n})$ is also applicable to practical sensor networks.

A general random intersection graph $\mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n)$ can also be used to model a social network, where a vertex represents an individual, and an object could be an hobby of individuals, a book being read, or a movie being watched, etc. Then a link between two people characterize a common-interest relation [3, 4, 6, 16, 26]; namely, two users have a connection if they have a common hobby, read a common book, or watch a common movie, etc. The heterogeneity of groups in $\mathbb{G}(n, \overrightarrow{\alpha}, \overrightarrow{K_n}, P_n)$ takes into account of the fact that users may have different number of interests. Our result shed light on the effect of heterogeneity on connectivity of a common-interest social network.

We organize the rest of the paper as follows. Section 2 presents some preliminaries. Afterwards, we detail the main result in Section 3. Subsequently, Sections 4 and 5 are devoted to proving the results. Section 6 surveys related work. Finally, we conclude the paper in Section 7.

2 Preliminaries

We notate the n vertices in graph $\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n)$ by $v_1, v_2, \ldots, v_n$; i.e., $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$. For each $x = 1, 2 \ldots, n$, the object set of vertex v_x is denoted by S_x. When v_x belongs to a group $\mathcal{A}_i$ for some $i \in \{1, 2, \ldots, m\}$, the set S_x is uniformly distributed among all $K_{i,n}$-size subsets of the object pool $\mathcal{P}_n$.

In graph $\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n)$, let E_{xy} be the event that two different vertices v_x and v_y have an edge in between. Clearly, E_{xy} is equivalent to the event $S_x \cap S_y \neq \emptyset$. To analyze E_{xy}, we often condition on the case where v_x belongs to group $\mathcal{A}_i$ and v_y belongs to group $\mathcal{A}_j$, where $i \in \{1, 2, \ldots, m\}$ and $j \in \{1, 2, \ldots, m\}$ (note that x and y are different, but i and j may be the same; i.e., different vertices v_x and v_y may belong to the same group).

Under $(v_x \in \mathcal{A}_i) \cap (v_y \in \mathcal{A}_j)$, vertex v_x has $K_{i,n}$ objects and vertex v_y has $K_{j,n}$ objects. Then it is clear that $\mathbb{P}[E_{xy} \mid (v_x \in \mathcal{A}_i) \cap (v_y \in \mathcal{A}_j)]$ depends on i and j, but does not rely on x and y, so we can define

$$p_{ij} = \mathbb{P}[E_{xy} \mid (v_x \in \mathcal{A}_i) \cap (v_y \in \mathcal{A}_j)]. \tag{3}$$

We compute the probability p_{ij} below. Let $T(K_{i,n}, P_n)$ be the set of all $K_{i,n}$-size subsets of the object pool $\mathcal{P}_n$. Under $(v_x \in \mathcal{A}_i) \cap (v_y \in \mathcal{A}_j)$, the set S_x (resp., S_y) is uniformly distributed in $T(K_{i,n}, P_n)$ (resp., $T(K_{j,n}, P_n)$). Let S_x^* be an arbitrary element in $T(K_{i,n}, P_n)$. Conditioning on $S_x = S_x^*$, the event $\overline{E_{xy}}$ (i.e., $S_x \cap S_y = \emptyset$) means $S_y \subseteq \mathcal{P}_n \setminus S_x^*$. Noting that there are $\binom{P_n}{K_{j,n}}$ ways to select a $K_{j,n}$-size set from $\mathcal{P}_n$ and there are $\binom{P_n - K_{i,n}}{K_{j,n}}$ ways to select a $K_{j,n}$-size set from $\mathcal{P}_n \setminus S_x^*$, we readily obtain

$$\mathbb{P}\left[\overline{E_{xy}} \mid (S_x = S_x^*) \cap (v_y \in \mathcal{A}_j)\right] = \frac{\binom{P_n - K_{i,n}}{K_{j,n}}}{\binom{P_n}{K_{j,n}}}. \tag{4}$$

From (3) and (4), it follows that

$$p_{ij} = \sum_{S_x^* \in T(K_{i,n}, P_n)} \left\{\mathbb{P}\left[S_x = S_x^*\right] \mathbb{P}\left[E_{xy} \mid (S_x = S_x^*) \cap (v_y \in \mathcal{A}_j)\right]\right\} = 1 - \frac{\binom{P_n - K_{i,n}}{K_{j,n}}}{\binom{P_n}{K_{j,n}}}, \tag{5}$$

where we use $\sum_{S_x^* \in T(K_{i,n}, P_n)} \mathbb{P}\left[S_x = S_x^* \mid v_x \in \mathcal{A}_i\right] = 1$.

Then we compute $b_{i,n}$ which denotes $\mathbb{P}[E_{xy} \mid (v_x \in \mathcal{A}_i)]$; i.e., the probability of v_x and v_y have an edge conditioning on the event that v_x belongs to group $\mathcal{A}_i$. Clearly, we have

$$\begin{aligned} b_{i,n} &= \mathbb{P}[E_{xy} \mid (v_x \in \mathcal{A}_i)] \\ &= \sum_{j=1}^{m} \left(\mathbb{P}\left[v_y \in \mathcal{A}_j\right] \mathbb{P}[E_{xy} \mid (v_x \in \mathcal{A}_i) \cap (v_y \in \mathcal{A}_j)]\right) \\ &= \sum_{j=1}^{m} \left(a_j p_{ij}\right). \end{aligned} \tag{6}$$

We can further compute $\mathbb{P}[E_{xy}]$. It follows that

$$\begin{aligned} \mathbb{P}[E_{xy}] &= \sum_{i=1}^{m} \left(\mathbb{P}\left[v_x \in \mathcal{A}_i\right] \mathbb{P}[E_{xy} \mid (v_x \in \mathcal{A}_i)]\right) \\ &= \sum_{i=1}^{m} \sum_{j=1}^{m} \left(a_i a_j p_{ij}\right). \end{aligned} \tag{7}$$

where the last step uses (6).

Our main result provided in the next section involves $b_{1,n}$ (see (8)), which is the probability that a typical vertex in group $\mathcal{A}_1$ has an edge with another typical vertex in $\mathcal{V}_n$. From (5) and (6) with $i = 1$, we obtain that $b_{1,n}$ equals the left hand side of (1).

3 The Main Result

We present the main result in Theorem 1 below.

Theorem 1 *Consider a general random intersection graph* $\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n)$ *under* $P_n = \Omega(n)$ *and* $\omega(1) = K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{m,n} = o(\sqrt{P_n})$. *If there exists a sequence* β_n *satisfying* $|\beta_n| = o(\ln n)$ *such that*

$$b_{1,n} = \frac{\ln n + \beta_n}{n}, \tag{8}$$

where $b_{1,n}$ *equals the left hand side of (1), then it holds that*

$$\lim_{n\to\infty} \mathbb{P}\Big[\begin{array}{c}\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n)\\ \textit{is connected.}\end{array}\Big] = \begin{cases} 0, & \textit{if } \lim\limits_{n\to\infty} \beta_n = -\infty, \quad (9a)\\ 1, & \textit{if } \lim\limits_{n\to\infty} \beta_n = \infty. \quad (9b)\end{cases}$$

In Section I, we have already discussed the result in Theorem 1; in particular, we explain therein that Theorem 1 gives a sharp zero-one law for connectivity in a graph $\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n)$. The next section presents the proof of Theorem 1.

4 Establishing Theorem 1

In proving Theorem 1, we use the relationship between connectivity and the absence of isolated vertex. It is easy to see that if a graph is connected, then it does not contain any isolated vertex [12]. Therefore, we immediately have

$$\mathbb{P}\Big[\,\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n) \text{ is connected.}\,\Big] \leq \mathbb{P}\Big[\begin{array}{c}\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n) \text{ contains}\\ \text{no isolated vertex.}\end{array}\Big] \tag{10}$$

and

$$\begin{aligned}&\mathbb{P}\Big[\,\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n) \text{ is connected.}\,\Big]\\ &= \mathbb{P}\Big[\begin{array}{c}\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n) \text{ contains}\\ \text{no isolated vertex.}\end{array}\Big] - \mathbb{P}\Big[\begin{array}{l}\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n) \text{ has no isolated vertex,}\\ \text{but is not connected.}\end{array}\Big]. \end{aligned}\tag{11}$$

Given (10) and (11), we will complete proving Theorem 1 once we establish Lemmas 1 and 2 below. In the rest of the paper, by "the conditions of Theorem 1", we mean $P_n = \Omega(n)$, $\omega(1) = K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{m,n} = o(\sqrt{P_n})$ and (8) (i.e., $b_{1,n} = \frac{\ln n + \beta_n}{n}$) with $|\beta_n| = o(\ln n)$.

Lemma 1 *For a graph* $\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n)$ *under the conditions of Theorem 1, it holds that*

$$\lim_{n\to\infty} \mathbb{P}\Big[\begin{array}{c}\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n) \textit{ contains}\\ \textit{no isolated vertex.}\end{array}\Big] = \begin{cases} 0, & \textit{if } \lim\limits_{n\to\infty} \beta_n = -\infty, \quad (12a)\\ 1, & \textit{if } \lim\limits_{n\to\infty} \beta_n = \infty, \quad (12b)\end{cases}$$

Lemma 1 presents a zero-one law on the absence of isolated vertex via (12a) and (12b). In the next subsection, we explain the idea of proving (12a) and (12b) by the method of moments.

Lemma 2 *For a graph* $\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n)$ *under the conditions of Theorem 1, it holds that*

$$\lim_{n\to\infty} \mathbb{P}\Big[\begin{array}{c}\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n) \textit{ has no isolated vertex,}\\ \textit{but is not connected.}\end{array}\Big] = 0. \tag{13}$$

Lemma 2 is established in Section 5.

4.1 Method of moments to prove Lemma 1 on the absence of isolated vertex

We use the method of moments [14, Page 55] to prove Lemma 1 on the absence of isolated vertex. Below we establish (12a) and (12b) of Lemma 1, respectively.

4.1.1 Establishing (12a)

We prove (12a) by the method of the first moment [14, Page 55] applied to the total number of isolated vertices in $\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n)$. With indicator variables $\phi_{n,i}$ for $i = 1, \ldots, n$ defined by

$$\begin{aligned}\phi_{n,i} &= \mathbf{1}\left[\text{Vertex } v_i \text{ is isolated in } \mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n).\right] \\ &= \begin{cases} 1, & \text{if } v_i \text{ is isolated in } \mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n), \\ 0, & \text{if } v_i \text{ is not isolated in } \mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n). \end{cases}\end{aligned}$$

then J_n denoting the number of isolated vertex in $\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n)$ is given by

$$J_n := \sum_{i=1}^{n} \phi_{n,i}.$$

The random graph $\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n)$ has no isolated vertex if and only if $J_n = 0$.

The method of first moment [14, Equation (3.10), Page 55] relies on the well-known bound

$$1 - \mathbb{E}\left[J_n\right] \leq \mathbb{P}\left[J_n = 0\right]. \tag{14}$$

Noting that the random variables $\phi_{n,1}, \ldots, \phi_{n,n}$ are exchangeable due to vertex symmetry, we find

$$\mathbb{E}\left[J_n\right] = n\mathbb{E}\left[\phi_{n,1}\right] \tag{15}$$

The desired one-law (12b) means $\lim_{n\to\infty} \mathbb{P}\left[J_n = 0\right] = 1$ under $\lim_{n\to\infty} \beta_n = \infty$. From (14) and (15), $\lim_{n\to\infty} \mathbb{P}\left[J_n = 0\right] = 1$ will be proved once we show

$$\lim_{n\to\infty} \left(n\mathbb{E}\left[\phi_{n,1}\right]\right) = 0. \tag{16}$$

Clearly, the event $(\phi_{n,1} = 1)$ (i.e., vertex v_1 is isolated) is equivalent to $\bigcap_{j=2}^{n} \overline{E_{1j}}$, where the event $\overline{E_{1j}}$ means that there is no edge between v_1 and v_j in graph $\mathbb{G}(n, \overrightarrow{a}, \overrightarrow{K_n}, P_n)$. Then

$$\begin{aligned}\mathbb{E}\left[\phi_{n,1}\right] &= \mathbb{P}\left[v_1 \text{ is isolated}\right] \\ &= \sum_{i=1}^{m} \mathbb{P}\left[v_1 \in \mathcal{A}_i\right] \mathbb{P}\left[v_1 \text{ is isolated} \mid v_1 \in \mathcal{A}_i\right] \\ &= \sum_{i=1}^{m} a_i \mathbb{P}\left[\cap_{j=2}^{n} \overline{E_{1j}} \mid v_1 \in \mathcal{A}_i\right] \end{aligned} \tag{17}$$

Recall that $T(K_{i,n}, P_n)$ is the set of all $K_{i,n}$-size subsets of the object pool $\mathcal{P}_n$. Conditioning on S_1, events $\overline{E_{1j}}|_{j=2,\ldots,n}$ are independent. Moreover, given any $S_1^* \in T(K_{i,n}, P_n)$, we note

$$\mathbb{P}\left[\overline{E_{1j}} \mid S_1 = S_1^*\right] = 1 - \mathbb{P}\left[E_{1j} \mid S_1 = S_1^*\right] = 1 - b_{i,n}, \quad \text{for } j = 2, \ldots, n. \tag{18}$$

where $b_{i,n}$ is given by (6). Hence, it holds that

$$\mathbb{P}\left[\cap_{j=2}^{n} \overline{E_{1j}} \mid v_1 \in \mathcal{A}_i\right] = \sum_{S_1^* \in T(K_{i,n}, P_n)} \mathbb{P}\left[S_1 = S_1^*\right] (1 - b_{i,n})^{n-1} = (1 - b_{i,n})^{n-1}, \tag{19}$$

where the last step uses $\sum_{S_1^* \in T(K_{i,n}, P_n)} \mathbb{P}\left[S_1 = S_1^* \mid v_1 \in \mathcal{A}_i\right] = 1$. Then the application of (19) to (17) yields

$$n\mathbb{E}\left[\phi_{n,1}\right] = n\sum_{i=1}^{m} a_i(1-b_{i,n})^{n-1} \leq n(1-b_{1,n})^{n-1}. \tag{20}$$

From (8) and $|\beta_n| = o(\ln n)$, it follows that

$$b_{1,n} \sim \frac{\ln n}{n} = o(1). \tag{21}$$

Then given $b_{1,n} = o(1)$ and ${b_{1,n}}^2 \cdot (n-1) \sim \left(\frac{\ln n}{n}\right)^2 \cdot (n-1) = o(1)$, we use [26, Fact 3] to derive

$$n(1-b_{1,n})^{n-1} \sim e^{-b_{1,n}(n-1)}. \tag{22}$$

Substituting (8) and $b_{1,n} = o(1)$ into (22), we obtain

$$n(1-b_{1,n})^{n-1} \sim ne^{-nb_{1,n}} \cdot e^{b_{1,n}} = ne^{-\ln n - \beta_n} \cdot e^{o(1)} \sim e^{-\beta_n}. \tag{23}$$

In view of (20) and (23), we conclude

$$n\mathbb{E}\left[\psi_{n,1}\right] \leq e^{-\beta_n} \cdot [1 + o(1)],$$

which implies (16). Then as explained above, (12a) is proved.

4.1.2 Establishing (12b)

We prove (12b) by the method of moments [14, Page 55] applied to the number of vertices that belong to group $\mathcal{A}_1$ and are isolated in $\mathbb{G}(n, \overrightarrow{d}, \overrightarrow{K_n}, P_n)$. With indicator variables $\psi_{n,i}$ for $i = 1, \ldots, n$ defined by

$$\begin{aligned}\psi_{n,i} &= \mathbf{1}\left[\text{Vertex } v_i \text{ belongs to group } \mathcal{A}_1 \text{ and is isolated in } \mathbb{G}(n, \overrightarrow{d}, \overrightarrow{K_n}, P_n).\right] \\ &= \begin{cases} 1, & \text{if } v_i \in \mathcal{A}_1 \textit{ and } v_i \text{ is isolated in } \mathbb{G}(n, \overrightarrow{d}, \overrightarrow{K_n}, P_n), \\ 0, & \text{if } v_i \notin \mathcal{A}_1 \textit{ or } v_i \text{ is not isolated in } \mathbb{G}(n, \overrightarrow{d}, \overrightarrow{K_n}, P_n). \end{cases}\end{aligned}$$

then I_n denoting the number of isolated vertex in $\mathbb{G}(n, \overrightarrow{d}, \overrightarrow{K_n}, P_n)$ is given by

$$I_n := \sum_{i=1}^{n} \psi_{n,i}.$$

From the method of second moment [14, Page 55], it follows that

$$\mathbb{P}\left[I_n = 0\right] \leq 1 - \frac{\mathbb{E}\left[I_n\right]^2}{\mathbb{E}\left[{I_n}^2\right]}. \tag{24}$$

Noting that the random variables $\psi_{n,1}, \ldots, \psi_{n,n}$ are exchangeable due to vertex symmetry, we find

$$\mathbb{E}\left[I_n\right] = n\mathbb{E}\left[\psi_{n,1}\right] \tag{25}$$

and

$$\begin{aligned}\mathbb{E}\left[{I_n}^2\right] &= n\mathbb{E}\left[{\psi_{n,1}}^2\right] + n(n-1)\mathbb{E}\left[\psi_{n,1}\psi_{n,2}\right] \\ &= n\mathbb{E}\left[\psi_{n,1}\right] + n(n-1)\mathbb{E}\left[\psi_{n,1}\psi_{n,2}\right],\end{aligned} \tag{26}$$

where the last step uses $\mathbb{E}\left[{\psi_{n,1}}^2\right] = \mathbb{E}\left[\psi_{n,1}\right]$ as $\psi_{n,1}$ is a binary random variable. It then follows from (25) and (26) that

$$\frac{\mathbb{E}\left[{I_n}^2\right]}{\mathbb{E}\left[I_n\right]^2} = \frac{1}{n\mathbb{E}\left[\psi_{n,1}\right]} + \frac{n-1}{n} \cdot \frac{\mathbb{E}\left[\psi_{n,1}\psi_{n,2}\right]}{\left(\mathbb{E}\left[\psi_{n,1}\right]\right)^2}. \tag{27}$$

The desired zero-law (12a) means $\lim_{n\to\infty}\mathbb{P}\left[I_n=0\right]=0$ under $\lim_{n\to\infty}\beta_n=-\infty$. From (24) and (26), we will obtain $\lim_{n\to\infty}\mathbb{P}\left[I_n=0\right]=0$ once deriving

$$\lim_{n\to\infty}\left(n\mathbb{E}\left[\psi_{n,1}\right]\right)=\infty \tag{28}$$

and

$$\frac{\mathbb{E}\left[\psi_{n,1}\psi_{n,2}\right]}{\left(\mathbb{E}\left[\psi_{n,1}\right]\right)^2}\leq 1+o(1). \tag{29}$$

The reason is that under (28) and (29), we apply them to (27) and derive $\frac{\mathbb{E}\left[{I_n}^2\right]}{\mathbb{E}\left[I_n\right]^2}\leq 1+o(1)$, implying $\frac{\mathbb{E}\left[I_n\right]^2}{\mathbb{E}\left[{I_n}^2\right]}\geq 1-o(1)$, which is used in (24) to establish $\lim_{n\to\infty}\mathbb{P}\left[I_n=0\right]=0$.

Below we prove (28) and (29), respectively.

Establishing (28):

Clearly, the event $(\psi_{n,1}=1)$ is equivalent to $(v_i\in\mathcal{A}_1)\cap\left(\cap_{j=2}^n\overline{E_{1j}}\right)$. Then

$$\begin{aligned}\mathbb{E}\left[\psi_{n,1}\right]&=\mathbb{P}\left[\psi_{n,1}=1\right]\\&=\mathbb{P}\left[(v_i\in\mathcal{A}_1)\cap(\cap_{j=2}^n\overline{E_{1j}})\right]\\&=\mathbb{P}\left[v_i\in\mathcal{A}_1\right]\mathbb{P}\left[\cap_{j=2}^n\overline{E_{1j}}\mid v_1\in\mathcal{A}_1\right]\\&=a_1\mathbb{P}\left[\cap_{j=2}^n\overline{E_{1j}}\mid v_1\in\mathcal{A}_1\right]\end{aligned} \tag{30}$$

From (19), we have

$$\mathbb{P}\left[\cap_{j=2}^n\overline{E_{1j}}\mid v_1\in\mathcal{A}_1\right]=\left(1-b_{1,n}\right)^{n-1}. \tag{31}$$

Then the use of (31) to (30) induces

$$\mathbb{E}\left[\psi_{n,1}\right]=a_1(1-b_{1,n})^{n-1}. \tag{32}$$

Furthermore, from (23) and (32), we derive

$$n\mathbb{E}\left[\psi_{n,1}\right]\sim a_1e^{-\beta_n}. \tag{33}$$

Since a_1 is a positive constant, (33) implies (28).

Establishing (29):

The event $\left(\psi_{n,1}=1\right)\ \cap\ \left(\psi_{n,2}=1\right)$ means that both vertices v_1 and v_2 belong to group $\mathcal{A}_1$ and are isolated in $\mathbb{G}(n,\overrightarrow{d},\overrightarrow{K_n},P_n)$. Then clearly event $\left(\psi_{n,1}=1\right)\ \cap\ \left(\psi_{n,2}=1\right)$ is given by $\left[\cap_{j=3}^n\left(\overline{E_{1j}}\cap\overline{E_{2j}}\right)\right]\cap(v_1\in\mathcal{A}_1)\cap(v_2\in\mathcal{A}_1)\cap\overline{E_{12}}$. Therefore, we have

$$\begin{aligned}&\mathbb{E}\left[\psi_{n,1}\psi_{n,2}\right]\\&\quad=\mathbb{P}\left[\left(\psi_{n,1}=1\right)\ \cap\ \left(\psi_{n,2}=1\right)\right]\\&\quad=\mathbb{P}\left[\left[\bigcap_{j=3}^n\left(\overline{E_{1j}}\cap\overline{E_{2j}}\right)\right]\cap(v_1\in\mathcal{A}_1)\cap(v_2\in\mathcal{A}_1)\cap\overline{E_{12}}\right]\\&\quad=\mathbb{P}\left[(v_1\in\mathcal{A}_1)\cap(v_2\in\mathcal{A}_1)\cap\overline{E_{12}}\right]\mathbb{P}\left[\left[\bigcap_{j=3}^n\left(\overline{E_{1j}}\cap\overline{E_{2j}}\right)\right]\mid(v_1\in\mathcal{A}_1)\cap(v_2\in\mathcal{A}_1)\cap\overline{E_{12}}\right].\end{aligned} \tag{34}$$

First, we get

$$\begin{aligned}&\mathbb{P}\left[(v_1\in\mathcal{A}_1)\cap(v_2\in\mathcal{A}_1)\cap\overline{E_{12}}\right]\\&\quad\leq\mathbb{P}\left[(v_1\in\mathcal{A}_1)\cap(v_2\in\mathcal{A}_1)\right]\\&\quad=\mathbb{P}\left[v_1\in\mathcal{A}_1\right]\mathbb{P}\left[v_2\in\mathcal{A}_1\right]\\&\quad={a_1}^2.\end{aligned} \tag{35}$$

Second, to evaluate $\mathbb{P}\left[[\bigcap_{j=3}^{n}\left(\overline{E_{1j}}\cap\overline{E_{2j}}\right)] \mid (v_1\in\mathcal{A}_1)\cap(v_2\in\mathcal{A}_1)\cap\overline{E_{12}}\right]$, we find it useful to define a set $\mathcal{L}(K_{1,n},P_n)$ as follows:

$$\mathcal{L}(K_{1,n},P_n)=\left\{(L_1,L_2)\mid \left(L_1\in T(K_{1,n},P_n)\right)\cap\left(L_2\in T(K_{1,n},P_n)\right)\cap\left(L_1\cap L_2=\emptyset\right)\right\}. \tag{36}$$

Then the event $(v_1\in\mathcal{A}_1)\cap(v_2\in\mathcal{A}_1)\cap\overline{E_{12}}$ is equivalent to the event that the vector (S_1,S_2) belongs to $\mathcal{L}(K_{1,n},P_n)$. Conditioning on S_1 and S_2, events $(\overline{E_{1j}}\cap\overline{E_{2j}})|_{j=3,\ldots,n}$ are independent. Hence, it becomes clear that

$$\begin{aligned}
&\mathbb{P}\left[\left[\bigcap_{j=3}^{n}\left(\overline{E_{1j}}\cap\overline{E_{2j}}\right)\right]\mid(v_1\in\mathcal{A}_1)\cap(v_2\in\mathcal{A}_1)\cap\overline{E_{12}}\right]\\
&\quad=\sum_{(S_1^*,S_2^*)\in\mathcal{L}(K_{1,n},P_n)}\left\{\mathbb{P}\left[(S_1=S_1^*)\cap(S_2=S_2^*)\right]\prod_{j=3}^{n}\mathbb{P}\left[\overline{E_{1j}}\cap\overline{E_{2j}}\mid(S_1=S_1^*)\cap(S_2=S_2^*)\right]\right\}.
\end{aligned}\tag{37}$$

As the above summation shows, (S_1^*,S_2^*) is an arbitrary element in $\mathcal{L}(K_{1,n},P_n)$.

For $j=3,\ldots,n$, we compute conditional probabilities when vertex v_j falls into a group $\mathcal{A}_\ell$ for some ℓ in $\{1,\ldots,n\}$, so it follows that

$$\begin{aligned}
&\mathbb{P}\left[\overline{E_{1j}}\cap\overline{E_{2j}}\mid(S_1=S_1^*)\cap(S_2=S_2^*)\right]\\
&\quad=\sum_{\ell=1}^{m}\left\{\mathbb{P}\left[v_j\in\mathcal{A}_\ell\right]\mathbb{P}\left[\overline{E_{1j}}\cap\overline{E_{2j}}\mid(S_1=S_1^*)\cap(S_2=S_2^*)\cap(v_j\in\mathcal{A}_\ell)\right]\right\}\\
&\quad=\sum_{\ell=1}^{m}\left\{a_\ell\,\mathbb{P}\left[\overline{E_{1j}}\cap\overline{E_{2j}}\mid(S_1=S_1^*)\cap(S_2=S_2^*)\cap(v_j\in\mathcal{A}_\ell)\right]\right\}.
\end{aligned}\tag{38}$$

From $(S_1^*,S_2^*)\in\mathcal{L}(K_{1,n},P_n)$, and the definitions of $\mathcal{L}(K_{1,n},P_n)$ and $T(K_{1,n},P_n)$, we have $|S_1^*|=K_{1,n}$, $|S_2^*|=K_{1,n}$ and $S_1^*\cap S_2^*=\emptyset$. Note that event $\overline{E_{1j}}\cap\overline{E_{2j}}$ means that vertex v_j has no edge with any of v_1 and v_2; i.e., S_j is a subset of $\mathcal{P}_n\setminus(S_1\cup S_2)$. Under $v_j\in\mathcal{A}_\ell$, it holds that $|S_j|=K_{\ell,n}$. Then conditioning on $(S_1=S_1^*)\cap(S_2=S_2^*)\cap(v_j\in\mathcal{A}_\ell)$, $\overline{E_{1j}}\cap\overline{E_{2j}}$ means that S_j is a $K_{\ell,n}$-size subset of $\mathcal{P}_n\setminus(S_1^*\cup S_2^*)$, which has $P_n-2K_{1,n}$ objects. Thus, we have

$$\mathbb{P}\left[\overline{E_{1j}}\cap\overline{E_{2j}}\mid(S_1=S_1^*)\cap(S_2=S_2^*)\cap(v_j\in\mathcal{A}_\ell)\right]=\frac{\binom{P_n-2K_{1,n}}{K_{\ell,n}}}{\binom{P_n}{K_{\ell,n}}}. \tag{39}$$

Substituting (38) and (39) into (37), we derive

$$\begin{aligned}
&\mathbb{P}\left[\left[\bigcap_{j=3}^{n}\left(\overline{E_{1j}}\cap\overline{E_{2j}}\right)\right]\mid(v_1\in\mathcal{A}_1)\cap(v_2\in\mathcal{A}_1)\cap\overline{E_{12}}\right]\\
&\quad=\left\{\sum_{\ell=1}^{m}\left[a_\ell\frac{\binom{P_n-2K_{1,n}}{K_{\ell,n}}}{\binom{P_n}{K_{\ell,n}}}\right]\right\}^{n-2}\sum_{(S_1^*,S_2^*)\in\mathcal{L}(K_{1,n},P_n)}\mathbb{P}\left[(S_1=S_1^*)\cap(S_2=S_2^*)\right]\\
&\quad=\left\{\sum_{\ell=1}^{m}\left[a_\ell\frac{\binom{P_n-2K_{1,n}}{K_{\ell,n}}}{\binom{P_n}{K_{\ell,n}}}\right]\right\}^{n-2},
\end{aligned}\tag{40}$$

where the last step applies $\sum_{(S_1^*,S_2^*)\in\mathcal{L}(K_{1,n},P_n)}\mathbb{P}\left[(S_1=S_1^*)\cap(S_2=S_2^*)\right]=1$.

Then we use (40) and (35) in (34) to establish

$$\mathbb{E}\left[\psi_{n,1}\psi_{n,2}\right]\le {a_1}^2\left\{\sum_{\ell=1}^{m}\left[a_\ell\frac{\binom{P_n-2K_{1,n}}{K_{\ell,n}}}{\binom{P_n}{K_{\ell,n}}}\right]\right\}^{n-2} \tag{41}$$

Then in view of (32) (41) and $\lim_{n\to\infty}(1-b_{1,n})=1$ from (21), we derive

$$\frac{\mathbb{E}\left[\psi_{n,1}\psi_{n,2}\right]}{\left(\mathbb{E}\left[\psi_{n,1}\right]\right)^2} \le \frac{{a_1}^2\left\{\sum_{\ell=1}^{m}\left[a_\ell\frac{\binom{P_n-2K_{1,n}}{K_{\ell,n}}}{\binom{P_n}{K_{\ell,n}}}\right]\right\}^{n-2}}{[a_1(1-b_{1,n})^{n-1}]^2} \le \left\{\frac{\sum_{\ell=1}^{m}\left[a_\ell\frac{\binom{P_n-2K_{1,n}}{K_{\ell,n}}}{\binom{P_n}{K_{\ell,n}}}\right]}{(1-b_{1,n})^2}\right\}^{n-2}\cdot[1+o(1)]. \tag{42}$$

In Appendix A of the online full version [25], we establish

$$\left\{\frac{\sum_{\ell=1}^{m}\left[a_\ell\frac{\binom{P_n-2K_{1,n}}{K_{\ell,n}}}{\binom{P_n}{K_{\ell,n}}}\right]}{\left\{\sum_{\ell=1}^{m}\left[a_\ell\frac{\binom{P_n-K_{1,n}}{K_{\ell,n}}}{\binom{P_n}{K_{\ell,n}}}\right]\right\}^2}\right\}^{n-2} \le [1+o(1)]. \tag{43}$$

Recalling the expression of $b_{1,n}$ in the left hand side of (1), we clearly obtain (29) from (42) and (43).

5 Establishing Lemma 2

For convenience, we use F_n to denote the event that graph $\mathbb{G}(n,\overrightarrow{d},\overrightarrow{K_n},P_n)$ has no isolated vertex, but is not connected. The basic idea to prove Lemma 2 is to find an upper bound on the probability $\mathbb{P}[F_n]$ and then to demonstrate that this bound converges to zero as $n\to\infty$.

We use $\mathcal{N}$ to denote the collection of all non-empty subsets of the vertex set $\{v_1,\ldots,v_n\}$. Similar to Yağan [21] and Zhao *et al.* [26], we set

$$r_n^* := \min\left(\left\lfloor\frac{P_n}{K_{1,n}}\right\rfloor,\ \left\lfloor\frac{n}{2}\right\rfloor\right).$$

and

$$X_{n,i}=\begin{cases}\max\{\lfloor(1+\varepsilon)K_n\rfloor,\lfloor\lambda K_{1,n}i\rfloor\} & \text{for } i=2,\ldots,r_n^*,\\ \lfloor\mu P_n\rfloor, & \text{for } i=r_n^*+1,\ldots,n,\end{cases} \tag{44}$$

for an arbitrary constant ε with $0<\varepsilon<1$, and some constants λ,μ that satisfy $0<\lambda<\frac{1}{2}$, $0<\mu<\frac{1}{2}$, and are selected to ensure [21, Equations (43) and (44)].

Then with $\boldsymbol{X}_n$ denoting the vector $(X_{n,1},\ X_{n,2},\ \ldots,\ X_{n,n})$, we define an event $E_n(\boldsymbol{X}_n)$ through

$$E_n(\boldsymbol{X}_n)=\bigcup_{T\subseteq\mathcal{N}:\ |T|\ge 2}\left[\left|\cup_{i\in T}S_i\right|\ \le\ X_{n,|T|}\right].$$

By a crude bounding argument, we get

$$\mathbb{P}[F_n]\le\mathbb{P}[E_n(\boldsymbol{X}_n)]+\mathbb{P}\left[F_n\cap\overline{E_n(\boldsymbol{X}_n)}\right].$$

From (45), a proof of Lemma 2 reduces to establishing the following two propositions.

Proposition 1 *Under the conditions of Theorem 1, it holds that*

$$\lim_{n\to\infty}\mathbb{P}[E_n(\boldsymbol{X}_n)]=0. \tag{45}$$

Proposition 2 *Under the conditions of Theorem 1, it holds that*

$$\mathbb{P}\left[F_n\cap\overline{E_n(\boldsymbol{X}_n)}\right]=o(1).$$

The proofs of Propositions 1 and 2 are given in Appendix B and Appendix C of the online full version [25], respectively.

6 Related Work

The general random intersection graph model $\mathbb{G}(n, \overrightarrow{d}, \overrightarrow{K}_n, P_n)$ is first studied by Godehardt and Jaworski [10], who give a result on the absence of isolated vertex. Afterwards, Goderhardt *et al.* [11] extend the result to connectivity. However, the results of both work [10, 11] require $P_n = O\left(\frac{n}{\log n}\right)$, which is not applicable to practical secure sensor networks, in which P_n grows at least linearly with the number of sensors n have reasonable resiliency against sensor capture attacks [7,21,26]. As proved by [7], P_n needs to be $\Omega(n)$ so that an adversary capturing $o(n)$ sensors can only compromise an $o(1)$ portion of sensor communications. In addition, Bloznelis *et al.* [5] investigate component evolution in $\mathbb{G}(n, \overrightarrow{d}, \overrightarrow{K}_n, P_n)$ and present conditions for the existence of a *giant component* (i.e., a connected component of $\Theta(n)$ vertices). Recently, Zhao *et al.* [29] consider k-connectivity of general random intersection graphs. Later, Yağan [20] shows that the result of Zhao *et al.* [29] is constrained to very narrow parameter ranges and is not applicable to real-world secure sensor networks. Yağan [20] establishes a zero-one law of connectivity in $\mathbb{G}(n, \overrightarrow{d}, \overrightarrow{K}_n, P_n)$. Specifically, recalling that $b_{1,n}$ is the probability that a typical vertex in group $\mathcal{A}_1$ has an edge with another typical vertex in $\mathcal{V}_n$ ($b_{1,n}$ equals the left hand side of (1), we rewrite Yağan's result as follows:

For a graph $\mathbb{G}(n, \overrightarrow{d}, \overrightarrow{K_n}, P_n)$ *under* $P_n = \Omega(n)$ *and* $\omega\left(\sqrt{\frac{P_n}{n}}\right) = K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{m,n} = o\left(\sqrt{\frac{P_n(\ln n)^2}{n}}\right)$, *if there exists a positive constant* c *such that*

$$b_{1,n} \sim \frac{c \ln n}{n}, \tag{46}$$

then it holds that

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{c}\mathbb{G}(n, \overrightarrow{d}, \overrightarrow{K_n}, P_n) \\ \textit{is connected.}\end{array}\right] = \begin{cases} 0, & \textit{if } c < 1, \\ 1, & \textit{if } c > 1. \end{cases} \tag{47}$$

However, as we explain below, our result outperforms Yağan's result [20] in the following two aspects. First, our zero-one law is more fine-grained than that of Yağan [20]. In a nutshell, with β_n given by (8), the scaling condition (46) enforced by Yağan [20] requires a deviation of $\beta_n = \pm\Omega(\ln n)$ to get the zero-one law, whereas in our formulation (8), it suffices to have an unbounded deviation; e.g., even $\beta_n = \pm\Theta(\ln n \ln n), \pm\Theta(\ln n \ln n \ln n)$ will do (note that Section 1 already has a discussion on this). Put differently, we cover the case of $c = 1$ in (47) under (46) and show that $\mathbb{G}(n, \overrightarrow{d}, \overrightarrow{K}_n, P_n)$ could be connected or disconnected with high probability, depending on the limit of β_n. Second, our condition $\omega(1) = K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{m,n} = o(\sqrt{P_n})$ is broader than the condition by Yağan [20]: $P_n = \Omega(n)$ and $\omega\left(\sqrt{\frac{P_n}{n}}\right) = K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{m,n} = o\left(\sqrt{\frac{P_n(\ln n)^2}{n}}\right)$, and thus has broader applicability in secure sensor networks and social networks. The first point (i.e., a more fine-grained zero-one law) of the two points above is the major improvement of our work over Yağan's result [20]. For a few other random graphs, this kind of improvement is the focus of several work [13, 15, 23, 24, 26, 27] as well.

7 Conclusion

In this paper, we derive a sharp zero-one law for connectivity in a general random intersection graph. Our result can be applied to secure sensor networks and social networks. A general random intersection graph is defined on a vertex set $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ as follows. Each vertex v_i ($i = 1, 2, \ldots, n$) is assigned an object set S_i from an object pool $\mathcal{P}_n$ comprising P_n distinct objects. Each object set S_i is formed according to the following two-step procedure: First, the size of S_i, $|S_i|$, is determined according to the following probability distribution $\mathbb{P}[v \in \mathcal{A}_i] = a_i$, where $\sum_{i=1}^{m} a_i = 1$. Next, S_i is constructed by selecting $|S_i|$ distinct objects uniformly at random from the object pool $\mathcal{P}_n$. This process is repeated independently for all object sets $S_1, \ldots, S_n$. Finally, an undirected edge is assigned between two vertices if and only if their corresponding object sets have at least one object in common; namely, distinct vertices v_i and v_j have an edge in between if and only if $S_i \cap S_j \neq \emptyset$.

References

[1] F. G. Ball, D. J. Sirl, and P. Trapman. Epidemics on random intersection graphs. *The Annals of Applied Probability*, 24(3):1081–1128, June 2014.

[2] S. Blackburn and S. Gerke. Connectivity of the uniform random intersection graph. *Discrete Mathematics*, 309(16), August 2009.

[3] M. Bloznelis. Degree and clustering coefficient in sparse random intersection graphs. *The Annals of Applied Probability*, 23(3):1254–1289, 2013.

[4] M. Bloznelis, J. Jaworski, and V. Kurauskas. Assortativity and clustering of sparse random intersection graphs. *The Electronic Journal of Probability*, 18(38):1–24, 2013.

[5] M. Bloznelis, J. Jaworski, and K. Rybarczyk. Component evolution in a secure wireless sensor network. *Networks*, 53:19–26, January 2009.

[6] M. Bradonjić, A. Hagberg, N. Hengartner, and A. Percus. Component evolution in general random intersection graphs. In *Workshop on Algorithms and Models for the Web Graph (WAW)*, pages 36–49, 2010.

[7] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan. Redoubtable sensor networks. *ACM Trans. Inf. Syst. Secur.*, 11(3):13:1–13:22, 2008.

[8] L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In *ACM Conference on Computer and Communications Security (CCS)*, 2002.

[9] V. Gligor, A. Perrig, and J. Zhao. Brief encounters with a random key graph. In B. Christianson, J. Malcolm, V. Maty, and M. Roe, editors, *Security Protocols XVII*, volume 7028 of *Lecture Notes in Computer Science*, pages 157–161. 2013.

[10] E. Godehardt and J. Jaworski. Two models of random intersection graphs for classification. In *Exploratory data analysis in empirical research*, pages 67–81. 2003.

[11] E. Godehardt, J. Jaworski, and K. Rybarczyk. Random intersection graphs and classification. In *Advances in data analysis*, pages 67–74. Springer, 2007.

[12] P. Gupta and P. R. Kumar. Critical power for asymptotic connectivity in wireless networks. In *Proc. IEEE CDC*, pages 547–566, 1998.

[13] G. Han and A. M. Makowski. A very strong zero-one law for connectivity in one-dimensional geometric random graphs. *IEEE Communications Letters*, 11(1):55–57, 2007.

[14] S. Janson, T. Łuczak, and A. Ruciński. *Random graphs*. Wiley-Interscience Series on Discrete Mathematics and Optimization, 2000.

[15] A. Makowski and O. Yağan. On the eschenauer-gligor key predistribution scheme under on-off communication channels: The absence of isolated nodes. In *Allerton Conference on Communication, Control, and Computing*, 2015.

[16] P. Marbach. A lower-bound on the number of rankings required in recommender systems using collaborativ filtering. In *IEEE Conference on Information Sciences and Systems (CISS)*, 2008.

[17] K. Rybarczyk. Diameter, connectivity and phase transition of the uniform random intersection graph. *Discrete Mathematics*, 311, 2011.

[18] K. Rybarczyk. Sharp threshold functions for the random intersection graph via a coupling method. *The Electronic Journal of Combinatorics*, 18:36–47, 2011.

[19] K. Rybarczyk. The coupling method for inhomogeneous random intersection graphs. *ArXiv e-prints*, January 2013. Available online at http://arxiv.org/abs/1301.0466

[20] O. Yagan. Zero-one laws for connectivity in inhomogeneous random key graphs. *ArXiv e-prints*, August 2015. Available online at http://arxiv.org/abs/1508.02407

[21] O. Yağan. Performance of the Eschenauer–Gligor key distribution scheme under an on/off channel. *IEEE Transactions on Information Theory*, 58(6):3821–3835, June 2012.

[22] O. Yağan and A. M. Makowski. Zero–one laws for connectivity in random key graphs. *IEEE Transactions on Information Theory*, 58(5):2983–2999, May 2012.

[23] F. Yavuz, J. Zhao, O. Yagan, and V. Gligor. Towards k-connectivity of the random graph induced by a pairwise key predistribution scheme with unreliable links. *IEEE Transactions on Information Theory*, 2015, forthcoming.

[24] F. Yavuz, J. Zhao, O. Yağan, and V. Gligor. On secure and reliable communications in wireless sensor networks: Towards k-connectivity under a random pairwise key predistribution scheme. In *IEEE International Symposium on Information Theory (ISIT)*, 2014.

[25] J. Zhao. On connectivity of a general random intersection graph. August 2015.

[26] J. Zhao, O. Yagan, and V. Gligor. k-Connectivity in random key graphs with unreliable links. *IEEE Transactions on Information Theory*, 61(7):3810–3836, July 2015.

[27] J. Zhao, O. Yağan, and V. Gligor. Secure k-connectivity in wireless sensor networks under an on/off channel model. In *IEEE International Symposium on Information Theory (ISIT)*, 2013.

[28] J. Zhao, O. Yağan, and V. Gligor. Connectivity in secure wireless sensor networks under transmission constraints. In *Allerton Conference on Communication, Control, and Computing*, 2014.

[29] J. Zhao, O. Yağan, and V. Gligor. On the strengths of connectivity and robustness in general random intersection graphs. In *IEEE Conference on Decision and Control (CDC)*, 2014.